METHOD FOR ASSIGNING ENCRYPTION KEYS

ABSTRACT OF THE DISCLOSURE

Sets of encryption keys useful by devices for decrypting encrypted content are defined using an error-correcting code such as a Reed-Solomon code to define vectors of length "n" over an alphabet of (0,...,N-1), wherein "n" is the number of columns in a key matrix and "N" is the number of rows in the matrix. Each vector represents a set of keys that can be assigned to a device. With this invention, overlap between sets of keys can be minimized to minimize the possibility that the key set of an innocent device might be inadvertently revoked when the key set of a compromised device is revoked. Also, only the generating matrix of the error-correcting code and the index of one set of keys need be stored in memory, since all previously defined key sets can be regenerated if need be from just the generating matrix and index.